AMENDMENTS TO THE CLAIMS

Applicants submit below a complete listing of the current claims, including marked-up claims with insertions indicated by underlining and deletions indicated by strikeouts and/or double bracketing. This listing of claims replaces all prior versions, and listings, of claims in the application:

Listing of the Claims

1.   (Currently amended) A computer-implemented method, comprising:

receiving, by an operating system and/or an enforcement module which is associated with or is part of the operating system, a call from an application via a first application programming interface, the call having parameters for a connection to an endpoint that the application desires to establish, whereby the application explicitly communicates a request to establish the connection;

receiving from the application via the first application programming interface a request to establish the connection;

providing the application with an indication indicating that the request is supported; and

making, by the operating system and/or the enforcement module, a call via a second application programming interface to a firewall to establish the connection in accordance with the parameters.

2.   (Original) The method of claim 1, further comprising, at the firewall, evaluating the parameters with respect to a policy and, if the parameters meet the policy, establishing the network connection in accordance with the parameters.

3.   (Original) The method of claim 1, wherein the parameters comprise a known endpoint to which the application would like to be connected.

4.   (Original)   The method of claim 3, wherein the parameters further comprise a request to limit the connection to a single connection.

5.   (Original)   The method of claim 4, further comprising, after the connection has been established, closing the connection in accordance with the request.

6.   (Previously presented)   The method of claim 1, wherein the parameters comprise a request for bandwidth or connection throttling for the connection.

7.   (Original)   The method of claim 1, wherein the parameters comprise limiting the connection to a subset of interfaces, local addresses, or remote addresses, or combinations thereof.

8.   (Original)   The method of claim 1, wherein the parameters comprise a timeout policy for the connection.

9.   (Original)   The method of claim 1, wherein the parameters comprise turning off or on specific protocol options.

10.   (Original)   The method of claim 1, wherein the parameters comprise information about a property of a flow that requires special handling.

11.   (Original)   The method of claim 10, wherein the information comprises a request for authentication or encryption.

12.   (Currently amended)   The method of claim 1, wherein the ~~indication comprises~~ application explicitly communicates the request to establish the connection by opening a listening socket.

13.   (Currently amended) The method of claim 1, wherein the ~~indication comprises~~ application explicitly communicates the request to establish the connection by connecting to a socket.

14.   (Original) The method of claim 1, wherein the call to the firewall is made via a firewall application programming interface.

15.   (Original) The method of claim 1, wherein the firewall is located on a computer with the application.

16.   (Original) The method of claim 1, wherein the firewall comprises an edge firewall, and further comprising an agent to communicate information to the edge firewall about the connection.

17.   (Original) The method of claim 1, wherein the firewall comprises an edge firewall, and further comprising an authenticated protocol to communicate information to the edge firewall about the connection.

18.   (Currently amended) A computer-storage~~readable~~ medium encoded with a computer program for performing the method recited in claim 1.

19.   (Currently amended) A computer system comprising:
an operating system;
[[an]] a first application programming interface associated with the operating system and configured and adapted to receive a call from an application, the call having parameters for a connection to an endpoint that the application desires to establish, whereby the application explicitly communicates a request to establish the connection; and
an enforcement module associated with the operating system and called via the application programming interface and configured and adapted to:

receive an indication from the application that the application desires to establish the connection; and

make a call via a second application programming interface to a firewall to establish the connection in accordance with the parameters.

20. (Original) The computer system of claim 19, further comprising a firewall application programming interface for making the call to the firewall.

21. (Currently amended) A computer-implemented method, comprising:

receiving, by an interception module including an application programming interface and a filter cache, a connect attempt, a listen attempt, or a combination thereof from an application or a service;

extracting, by the interception module, user and application or service information from the connect attempt, the listen attempt, or the combination thereof;

identifying, by the interception module, a user and the application or the service from the user and application or service information;

~~determining if the connect attempt, the listen attempt, or the combination thereof need to match a policy;~~

~~if the connect attempt, the listen attempt, or the combination thereof need to match the policy, establishing, via an application programming interface, the policy and adding the policy to a plurality of policies;~~

evaluating, by the interception module, the application or service information to determine if the connect attempt, the listen attempt, or the combination thereof comply with one or more policies from [[the]] a plurality of policies; and

if the connect attempt, the listen attempt, or the combination thereof comply with one or more policies from the plurality of policies, ~~configuring~~ instructing, by the interception module, a firewall to create a configuration to allow the connect attempt, the listen attempt, or the combination thereof, and storing the configuration in the filter cache.

22.   (Previously presented) The method of claim 21, further comprising if the connect attempt, the listen attempt, or the combination thereof do not comply with one or more policies from the plurality of policies, sending a notification to the user of the application or service.

23.   (Previously presented) The method of claim 22, wherein the notification comprises a selection to allow a connection.

24.   (Previously presented) The method of claim 21, wherein establishing the policy comprises receiving a policy from the application or service.

25.   (Previously presented) The method of claim 24, wherein receiving the policy comprises receiving the policy via the application programming interface.

26.   (Original) The method of claim 24, wherein the policy received from the application or service comprises inbound or outbound restrictions using one or more Internet Protocol addresses, information about a subnet, information about scope of the connection, or combinations thereof.

27.   (Original) The method of claim 24, wherein the policy received from the application or service comprises communication security level.

28.   (Original) The method of claim 27, wherein the communication security level comprises authentication.

29.   (Original) The method of claim 27, wherein the communication security level comprises encryption.

30.   (Original) The method of claim 21, wherein the firewall comprises a host firewall located on a computer with the application.

31.   (Original)   The method of claim 21, wherein the firewall comprises an edge firewall, and further comprising an agent to communicate information about the connection.

32.   (Original)   The method of claim 21, wherein the firewall comprises an edge firewall, and further comprising an authenticated protocol to communicate information to the edge firewall about the connection.

33.   (Currently amended)   A computer-storage~~readable~~ medium encoded with a computer program for performing the method recited in claim 21.

33-36. (Canceled)

37.   (Currently amended) A computer system, comprising:

a firewall; and

an interception module including an application programming interface and a filter cache and configured and adapted to:

intercept a request for a connect attempt, a listen attempt, or a combination thereof from an application or a service;

extract user and application or service information from the connect attempt, the listen attempt, or the combination thereof;

identify a user and the application or the service from the user and application or service information;

~~determine if the connect attempt, the listen attempt, or the combination thereof need to match a policy;~~

~~if the connect attempt, the listen attempt, or the combination thereof need to match the policy, establish, via the application programming interface, the policy and add the policy to a plurality of policies;~~

evaluate the application or service information to determine if the connect attempt, the listen attempt, or the combination thereof comply with one or more policies from [[the]] a plurality of policies; and

if the connect attempt, the listen attempt, or the combination thereof comply with one or more policies from the plurality of policies, ~~instruct~~ instructing the firewall to create a configuration to allow the connect attempt, the listen attempt, or the combination thereof, and storing the configuration in the filter cache.

38.   (Previously presented)   The computer system of claim 37, wherein the interception module comprises a policy cache for storing the plurality of policies.

39.   (Previously presented) The computer system of claim 37, wherein the interception module comprises a firewall client for communicating information about the connect attempt, the listen attempt, or the combination thereof to an edge firewall.